Halil, Defne; Kollnig, Konrad; Tamò-Larrieux, Aurelia

Article

Regulating pressing systemic risks: But not too soon?

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Halil, Defne; Kollnig, Konrad; Tamò-Larrieux, Aurelia (2025) : Regulating pressing systemic risks: But not too soon?, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 14, Iss. 2, pp. 1-29, https://doi.org/10.14763/2025.2.2010

This Version is available at:
https://hdl.handle.net/10419/321977

INTERNET POLICY REVIEW

Volume 14 **Issue** 2

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Regulating pressing systemic risks – but not too soon?

Defne Halil *Maastricht University*
Konrad Kollnig *Maastricht University*
Aurelia Tamò-Larrieux *University of Lausanne*

DOI: https://doi.org/10.14763/2025.2.2010

Published: 25 June 2025
Received: 17 September 2024 **Accepted:** 5 May 2025

Funding: Defne Halil received funding from Maastricht University's MaRBLe excellence programme. Konrad Kollnig has been supported by the RegTech4AI AiNed Fellowship Grant, which is funded by Dutch National Growth Fund (NGF) under file number NGF.1607.22.028.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Halil, D., Kollnig, K., & Tamò-Larrieux, A. (2025). Regulating pressing systemic risks – but not too soon? *Internet Policy Review*, *14*(2). https://doi.org/10.14763/2025.2.2010

Keywords: Digital Services Act (DSA), Data access requests, Digital services coordinators

Abstract: Online platforms have transformed how we live. This has raised concerns around how such platforms impact citizens' constitutionally-protected rights and freedoms, such as the freedom of expression and information, right to privacy, and protection from discrimination. To hold online platforms to account, researchers need access to platform data but this has proved to be difficult in the past. In response, the EU's 2022 Digital Services Act (DSA) imposes explicit obligations on very large online platforms (VLOPs) and very large online search engines (VLOSEs) to provide "vetted researchers" with necessary data to study systemic risks facilitated by these platforms. In this paper, we analyse how the platform data access provisions of the DSA work in practice and show the results of 27 data access requests launched across all EU member states. The results show that while the willingness of policymakers to address systemic risks on platforms is clearly present, we are not yet able to obtain meaningful data for research. In fact, the process of ensuring such access has been repeatedly delayed by the responsible authorities. For example, one authority claimed that requests not written in its national language would violate its country's procedural law and were thus not admissible. This is arguably not in line with the urgency required to address prevalent systemic risks, especially in a pivotal election year like 2024, the year when the study was conducted.

1. Introduction

Online platforms like Amazon, YouTube, and Instagram have revolutionised information sharing, communication, and commerce (Swan, 2022). While these platforms offer numerous benefits to society, concerns persist regarding user safety, particularly *systemic risks* imposed upon individuals online, such as the dissemination of illegal content, political polarisation, and disinformation (Kira, 2024). Given these potential risks, it is important for researchers, civil society, and authorities to have accessible means to hold online platforms to account and monitor potential risks. Given the data-driven nature of these online platforms, such independent accountability usually relies on voluntary access to data, too (European Digital Media Observatory, 2022). This, however, remains very challenging for researchers in practice (Van Drunen & Noroozian, 2024; Kollnig & Shadbolt, 2023). To date, the paradigm has been one where platforms have operated on highly criticised voluntary initiatives for data sharing (Darius & Stockmann, 2023). Only in August 2024, a few months before the US presidential elections, Meta closed down CrowdTangle, which used to be one of the primary tools for researchers to understand misinformation and election interference on Facebook; while there exists a replacement tool, this has been deemed inferior in many ways (Gotfredsen & Dowling, 2024). Twitter (now X) previously also offered a free research API that was widely used by academics to study topics such as misinformation, social psychology, and emergency management. Nonetheless, following Elon Musk's acquisition of the platform in 2023, access to the API was restricted and replaced with paid tiers. The new Enterprise access level of X costs around USD 42,000 per month, an amount that is very expensive for most publicly funded researchers (Murtfeldt et al., 2024). TikTok's Research API has also faced criticism due to several limitations, including data inaccuracies, strict restrictions on data retention, sharing, and licensing under its Terms of Service. These constraints have posed significant challenges for researchers, making it difficult to conduct reliable analyses, track data over time, or share findings for independent publication (Bekavac et al., 2024; Brown, 2023). This underlines that online platforms are unlikely, by themselves, to give researchers access to necessary data to study and mitigate systemic risks arising from online platforms.

To mitigate potential systemic risks arising from online platforms, the EU adopted the Digital Services Act (DSA) in 2022. The law became fully applicable more than a year ago, in February 2024. Large intermediary services, such as dominant social media platforms, search engines, and media services, are seen most likely to create systemic risks due to their large user base and intrinsic characteristics (Eder, 2023).

Therefore, those Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), that is, platforms that reach more than 45 million monthly active users in Europe, bear the most stringent obligations, as per Recital 76 of the DSA. Once officially recognised as such by the European Commission, these VLOPs and VLOSEs are granted four months to fulfil their obligations, as per Article 33(6) of the DSA. According to European Commission information last updated in February 2025, there are currently 23 VLOPs and two VLOSEs (European Commission, 2024b). The designated VLOPs are AliExpress, Amazon Store, Apple App Store, Pornhub, Booking.com, Google Play, Google Maps, Google Shopping, YouTube, Shein, LinkedIn, Facebook, Instagram, XNXX, Pinterest, Snapchat, Stripchat, TikTok, X, Temu, XVideos, Wikipedia, Zalando. And the VLOSEs are Google Search and Bing. WhatsApp is also expected to be designated as a VLOP, according to media reports citing a European Commission spokesperson, who confirmed that the service exceeds DSA's threshold of 45 million users (Datta, 2025).

Article 40 (4) of the DSA represents a significant step forward to platform governance by allowing "*vetted researchers*" to file platform data access requests and obtain access to *non-public* data to study systemic risks emerging from VLOPs and VLOSEs. Researchers must first submit the request to the respective Digital Services Coordinator (DSC). After scrutinising the data access request, the DSC will submit it to the relevant VLOP or VLOSE, which may approve the request or suggest an amendment to it. Such requests for non-public platform data promise to facilitate thorough academic inquiry, foster transparency, and promote public debate, which, according to scholars, would not be entirely feasible with only publicly available platform data (Engler, 2021).

Various initiatives have already been trying to monitor the implementation of the DSA in practice. For instance, AlgorithmWatch, a non-profit research and advocacy organisation, has launched an online form known as the "Systemic risk repository" (AlgorithmWatch, 2024). This platform allows individuals to submit real cases of systemic risks online or evidence of risks which have been mitigated. Additionally, the form seeks experts to help define what constitutes systemic risks. AlgorithmWatch also supports researchers and journalists in drafting and submitting their own data access requests (Marsh, 2024). In another effort, the DSA Observatory, a project run by the Institute for Information Law and University of Amsterdam, provides a regular analysis of the DSA through panels, articles, blog posts, expert workshops and conferences (DSA Observatory, 2024). TechPolicy, a non-profit organisation, has contributed by creating a comprehensive report in the form of a table outlining various platforms' data access mechanisms which exist beyond

the one specified under Article 40(4) of the DSA (Miller, 2024). That report outlines who has access to the specific platforms' data, whether an application is required, and whether a data dictionary is available. Moreover, the law firm, Bird & Bird, has created a DSA Implementation Tracker. This tool tracks the appointments of all the national DSCs, and the appointment of trusted flaggers and out-of-court dispute settlement bodies (Bird & Bird, 2024).

Building on these research and inquiry efforts, this paper explores the practicalities of how Article 40(4) of the DSA is being implemented across the EU by creating and sending data access requests on the systemic risk of illegal content. This provides a concrete understanding of how the DSCs currently interpret and manage those requests, which highlights certain challenges in the decentralised implementation of the DSA. We aim to lay the groundwork for future research on the societal impact of VLOPs and VLOSEs and provide initial insights on how the data access request mechanism is currently being operationalised across all EU member states. This is especially timely and pertinent given the decentralised nature of VLOPs within the EU and the possibility of divergent implementation of the DSA among EU member states (Van Drunen & Noroozian, 2024).

Concretely, we seek to address the research question: *How is Article 40 of the DSA, which grants access to non-public data held by VLOPs to vetted researchers, currently implemented across the EU?*

To study this research question, we first developed a standardised template for data access requests that adheres to the requirements delineated under Article 40(4)–(9) of the DSA (see Annex). Second, we sent real data access requests to all 27 DSCs established in the EU. These target only VLOPs and exclude VLOSEs as certain specific obligations related to illegal content, the main denominator of the requests, do not apply to VLOSEs (Wilman, 2022).

The data access requests of this study were sent out between March and June 2024, as the DSA became fully applicable in February 2024, according to Article 93(2) of the DSA. Thirdly, we evaluate the results from this empirical study, and make recommendations on how the DSA can be strengthened in practice.

It is important to mention that the complete framework for data access requests remains currently unavailable for researchers, as the forthcoming Delegated Act on data access requests, which will supplement the DSA, is not in force yet (European Commission, 2023a).

Initially, the Delegated Act was supposed to be adopted in the first quarter of 2024 (European Commission, 2023a). Nevertheless, according to a recent release by the German Federal Office, the Delegated Act is expected in early 2025 (German Federal Office, 2024). In October 2024, the draft Delegated Act was published by the European Commission, which followed with rounds of feedback. As of May 2025, the Delegated Act is still not adopted (European Commission, 2023a).

Arguably, the continued delay is becoming a significant impediment to fundamental rights protection in the EU, severely holding back platform accountability. With each passing month, the continued inaction intensifies existing risks and underscores the urgency of ensuring the effective implementation of Article 40 DSA. Among the most pressing challenges, as presented in the DSA risk assessment reports, are the persistent shortcomings in moderating disinformation, negative impacts on child safety, and the algorithmic biases affecting vulnerable communities (Hohlfeld, 2025). A concrete example is the 2024 Romanian presidential election: here, one candidate reportedly benefited from a coordinated Russian disinformation campaign via TikTok, prompting the annulment of this election by the Romanian Supreme Court. While researchers sought to investigate this incident through data access provisions under Article 40 of the DSA, their efforts were significantly challenged due to the delay in the law's implementation (Goanta et al., 2025).

The rest of this paper is structured as follows. First, we give an overview of Article 40(4) of the DSA framework and present the approach undertaken by this study to data access requests. We then report on the obtained data and analyse the responses. Lastly, we discuss our results, and provide directions for how the data access regime under Article 40(4) of the DSA can be strengthened in the future.

2. Getting access to data from VLOPs and VLOSEs by researchers

Access to non- public data from VLOPs and VLOSEs for research purposes regarding systemic risks, according to Article 40(4) of the DSA, is restricted to vetted researchers. To attain the designation of a vetted researcher, persons must demonstrate their affiliation with a university, non-academic research institute, or civil society organisation conducting scientific research, with the primary goal of supporting their public interest mission, as per Article 40(8) of the DSA. Vetted researchers must not have commercial interests, as there is a danger of commercial utilisation eclipsing public interest applications (Leerssen, 2021). Moreover, researchers seeking access to such non-public VLOP and VLOSE data must first, in accordance with Article 40(8) of the DSA, submit an application to the DSC, or in

other words, the national authority responsible for those matters.

The relevant DSC can be that of either the jurisdiction where the VLOP or VLOSE under research is based, or the EU member state authority of the research organisation to which the researcher is affiliated (Jaursch, 2024). Should researchers submit an application to the DSC of their EU member state, that DSC will forward the application, along with an initial evaluation, to the DSC for the establishment of the service. The role of the latter DSC, as per Article 40(9) of the DSA, is then to assess the researcher's application and either approve or reject it. This vetting process aims to establish whether researchers are vetted researchers based on the factors outlined in Article 40(8) of the DSA, such as their affiliation with a research organisation, independence from commercial interests, proof of research funding, capability to secure the data, demonstration proving that the requested data and time frames requested are necessary, and commitment to make the research publicly available. Additionally, as outlined in Article 40(4) of the DSA, the DSC must determine whether the data is requested for the "*sole purpose of contributing to the detection, identification and understanding of systemic risks…and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35*".

Per Article 49 of the DSA, DSCs are independent authorities responsible for matters relating to the supervision and enforcement of the DSA in the EU member states (Flew & Martin, 2022). Following Articles 53, 51, and 60 of the DSA, the DSCs can receive complaints, impose sanctions, and investigate. Most importantly, however, they are designated with exclusive jurisdiction over a provider that is established in their EU member state, as set forth in Article 56(1) of the DSA. Per Recital 123 of the DSA, the main establishment denotes the headquarters or registered office of a VLOP and VLOSE, where the key financial operations and control are centralised. The selection of the DSC is entrusted to the discretion of each EU member state, which may opt to set up an entirely new body or task an existing regulator with assuming the additional role of DSC. EU member states have been more inclined to set an existing regulator to take on the additional DSC role (Jaursch, 2022). Those authorities had to be appointed by each EU member state by 17 February 2024, in accordance with Article 49(3) of the DSA.

Turning back to the examination of the data access process: if the relevant DSC approves the researcher's application and grants them a "*vetted*" status, the DSC submits the data access request to the relevant VLOP or VLOSE which has 15 days to respond to it, in compliance with Article 40(5) of the DSA. The DSC with this submission must also specify the "*appropriate interfaces*", or in other words, how the

data must be shared by the VLOP or VLOSE to respect the requirements of Article 40(8) of the DSA. The VLOP or VLOSE may either approve the request or suggest an amendment. An amendment to the request, in line with Article 40(5) of the DSA, may be requested if the platform does not have access to such data or the data is confidential information, such as a trade secret (Synodinou et al., 2020).

If the platform suggests an amendment, it must propose alternative options of providing access to data, which can include suggestions of other types of data that satisfy the first request's research purpose, according to Article 40(6) of the DSA (Albert, 2022). In such instances, it is conceivable that the VLOPs and VLOSEs may choose not to furnish data by asserting that the information is unnecessary for evaluating systemic risks or implementing mitigation measures. Then, as per Article 40(6) of the DSA, the DSC is afforded 15 days, during which they must either approve or reject the said amendment. Ultimately, if there is initial approval or approval after the amendment, the VLOP or VLOSE must share the data with the researchers.

The upcoming Delegated Act on data access requests to be adopted by the Commission will provide more details on the main conditions for accessing non-public data set out in Article 40(13) of the DSA. Section 5 of this paper will delve deeper into the intricacies of the Delegated Act.

3. Understanding pressing systemic risks by means of data access requests

VLOPs and VLOSEs have obligations to assess and mitigate systemic risks in line with Articles 34 and 35 of the DSA. Despite the absence of an explicit definition of systemic risks in the DSA, Article 34 and Recitals 79–83, explicitly mention four categories of systemic risks that can occur: the dissemination of illegal content, the negative effects on the exercise of fundamental rights, the adverse effect on democratic processes, civic discourse and electoral processes, and public security, and negative effects on public health, minors, individual's physical and mental well-being, or instances of gender-based violence. The DSA is concerned with those systemic risks that originate from the operation of VLOPs and VLOSEs, particularly user behaviour and the platforms' own features (Eder, 2023). The severity and type of those risks can vary depending on which of these sources is involved. As mentioned in Section 2, the DSA provides vetted researchers with data access rights to study these systemic risks and how they are addressed by VLOPs and VLOSEs. Yet, as it stands, it is unclear how these data access rights will work in practice across the different member states of the EU and their respective DSCs.

To study our research question and understand how different DSCs handle Article 40(4) data requests, we sent exemplary data requests to all 27 DSCs established in the EU. We selected six VLOPs with different countries of establishment in the EU, namely, AliExpress (Netherlands), Amazon (Luxembourg), Zalando (Germany), YouTube (Ireland), Pornhub (Cyprus), and XVideos (Czech Republic), to enable comparative research to be conducted.

Additionally, we considered one VLOP that was not established in the EU at the time of sending the requests, namely Wikipedia. In this case, on the Commission's website, each VLOP listed was associated with a specific DSC, however, for Wikipedia it was indicated that any DSC is responsible (European Commission, 2024b). We selected the 21 remaining DSCs and sent the same requests to them. While we acknowledge that sending out similar requests to DSCs potentially creates duplicate work, our approach is nonetheless needed and legitimised by the pressing need of the research community to understand how the DSA works in practice. In terms of systemic risk, we focused on the moderation of illegal content by the VLOPs, a key concern of the DSA and a systemic risk that concerns all the selected VLOPs.

To keep the data access requests as similar as possible, the substance of our data access requests concerned the analysis of systemic risks arising from the dissemination of illegal content and its moderation, a category of risk that not only concerts all the selected VLOPs, but also represents a lowest common denominator for VLOPs among the systemic risks identified in the DSA (see Annex). The data access requests were adopted in the form of letters dispatched to the respective DSCs concurrently *via* their general email addresses as listed on their websites, or webforms when such were not present.

The first segment of the requests endeavoured to establish our status as vetted researchers, by a detailed demonstration of affiliation with a university and commitment to make the research publicly available and free of charge. It was specified that the funding for the research comes from our public research university (Van Hoboken et al., 2023). Those statements were substantiated by firstly annexing proof of university employment of one of the supervisors of this paper to the DSCs, and secondly, by proving his affiliation with the research lab of the university.

Our data access requests also incorporated our assurance of data security and confidentiality through the provision of a data management plan. This was done to ensure that the data requested is secured as far as it is necessary and proportionate for this research. Collaboratively created with the Data Stewardship Services of

the University, the data management plan stated that the data requested from the VLOPs will be stored in data storage provided by the University in line with its Data Management Code of Conduct. Additionally, the plan stipulated the retention of data for a minimum duration of ten years after the conclusion of the research endeavour. This retention period is in line with the country's Code of Conduct for Research Integrity and the Association of Universities. The data management plan received approval from the University's Data Protection Officer.

Secondly, a section labelled "*Research*" in the data access requests elucidated the research question of our study and how the data requested will contribute to the detection, identification, and understanding of systemic risks pursuant to Article 34(1) of the DSA in relation to the dissemination of illegal content. For instance, it was argued in the data access requests that the requested data related to user interaction with illegal content and geographic information is essential for understanding systemic risks for several reasons: regional variation in illegal content, analysing cultural sensitivity, and identification of emerging threats. Moreover, the data access requests explained that the research will contribute to the assessment of adequacy, efficiency, and impacts of the risk mitigation measures taken under Article 35 of the DSA by assessing measures implemented by VLOPs to mitigate the identified systemic risk. This is because the types of requested data related to content moderation practices of the selected VLOPs regarding illegal content. For example, it was stated in the data access requests that the requested data regarding the median time and tools for content moderation of illegal content depending on the categorisation provided by the VLOP is essential for assessing the mitigation measures taken by VLOPs. The subsequent section of the data access requests underscored the necessity and proportionality of the requested data *vis-à-vis* the paper's research objectives. The requests asserted the absence of personal or sensitive data requisition, emphasising that the requested data is not publicly available and cannot fall within the ambit of a trade secret. For example, it was stated that certain statistical data on illegal content remains absent from the Transparency Reports of the VLOPs and is thus non-public (Miller, 2023). An argument was made that the benefits derived from analysing and understanding illegal content outweigh data retention by the platforms.

Lastly, each data access request contained a list of all the types of data requested from the VLOPs. Only statistical data was requested and for the years 2018–2024, which is a time frame selected with careful consideration as not too short or long for our intended research. The starting point of 2018 was chosen as it marks the adoption of the Commission Recommendation 2018/334 on measures to effective-

ly tackle illegal content online, which can arguably be seen as the predecessor to the DSA's obligations regarding illegal content (European Union, 2025). This makes 2018 a logical baseline for examining how VLOP's practices evolved in response to increasing regulation. Extending the time frame to 2024 enables the inclusion of the most recent available data. This range also allows for an assessment of whether data access requests under the DSA can include data from before the DSA was adopted.

The following types of data were requested by the VLOPs: comprehensive breakdown of illegal content percentages (by type of illegal content), annual takedown numbers categorised by type of illegal content, number of notices submitted by trusted flaggers, the categorisation of those notices based on specific categories of illegal content, the median time for removal of illegal content using automatic or non-automatic tools, user interactions with illegal content, views on products associated with illegal items, and geographic information linked to the upload or creation of illegal content.

4. The responses from the DSCs: regulating systemic risks, but not now

Table 1 summarises the timing of the requests and responses by DSC. The first step to initiate a data access request is sending out the request to the responsible DSCs. The first batch of data access requests for this study were sent out on 7 March 2024, weeks after all the DSCs should have been designated, namely 17 February 2024. The second batch of data access requests, only aimed at Wikipedia, was sent out on 26 June 2024. None of the authorities actually provided us with data, even though the DSA has technically been in force since February 2024. Nevertheless, the study proceeds to contrast the responses to the requests by the DSCs even in the current circumstances as of late September 2024, from which recommendations for improving Article 40(4) of the DSA can be derived.

TABLE 1: Overview of the responses of the 27 EU member states. Country names are abbreviated using the established I
NA means non-applicable.

TOPIC	DATE OF SENDING DAR	RESPONSE DATE OF DSC	DID THE DSC STATE THEY WILL PROCESS THE DAR?	REPLIED IN ENGLISH OR THE NATIVE LANGUAGE?	STATEMENT BY DSC THAT DAR HAD TO BE SUBMITTED IN NATIONAL LANGUAGE	STATED THAT THEY WERE WAITING FOR THE DELEGATED ACT BEFORE PROCESSING DAR	FORMAT OF RESPONSE	WAS FURTHER PROCESSING DENIED DUE TO WIKIPEDIA BEING ESTABLISHED IN ANOTHER MS?	I
SL	26.06.24	10.07.24	NO	EN	**YES**	NO	EMAIL	YES	
SK	26.06.24	09.07.24	NO	EN	NO	NO	EMAIL AND SIGNED PDF	YES	
SE	26.06.24	28.06.24	**FIRST YES, THEN NO**	EN	NO	NO	EMAIL	YES (2ND REPLY)	
RO	26.06.24	**NO REPLY**	NA	NA	NA	NA	NA	NA	
PT	26.06.24	26.06.24	NO	EN	NO	NO	EMAIL	YES	
PL	26.06.24	18.09.24.	NO	EN	NO	NO	EMAIL AND PDF	NO	
NL	07.03.24	03.04.24	NO	EN	NO	YES	EMAIL	NA	
MT	26.06.24	01.07.24	**FIRST YES, THEN NO**	EN	NO	NO	EMAIL	YES (2ND REPLY)	
LV	26.06.24	09.07.24	NO	EN	NO	NO	EMAIL AND PDF	YES	
LU	07.03.24	19.03.24	**FIRST YES, THEN NO**	EN	NO	YES	EMAIL	NA	
LT	26.06.24	16.07.24	NO	EN	NO	YES	EMAIL AND PDF	YES	
IT	26.06.24	26.06.24	NO	EN	NO	NO	EMAIL	NO	
IE	07.03.24	08.03.24	NO	EN	NO	YES	EMAIL	NA	
HU	26.06.24	26.07.24	NO	**HU**	NO	NO	EMAIL	YES	

HR	26.06.24	30.07.24	NO	EN	NO	NO	EMAIL	YES
FR	26.06.24	28.08.24	NO	EN	NO	YES	EMAIL	YES
FI	26.06.24	16.07.24	NO	EN	NO	NO	EMAIL	YES
ES	26.06.24	26.09.24	NO	EN	NO	NO	EMAIL	YES
EL	26.06.24	30.08.24	NO	EN	NO	YES	EMAIL AND PDF	YES
EE	26.06.24	27.06.24	NO	EN	NO	NO	EMAIL	YES
DK	26.06.24	28.06.24	NO	EN	NO	YES	EMAIL	NO
DE	07.03.24	14.03.24	NO	EN	NO	YES	EMAIL	NA
CZ	07.03.24	04.04.24	NO	EN	NO	YES	EMAIL	NA
CY	07.03.24	**NO REPLY**	NA	NA	NO	NA	NA	NA
BG	26.06.24	09.07.24	NO	EN	NO	YES	EMAIL WITH SIGNED PDF STAMP	NO
BE	26.06.24	27.06.24	NO	EN	NO	NO	EMAIL	YES
AT	26.06.24	28.06.24	NO	EN	NO	YES	EMAIL AND PHONE	YES

25 out of 27 national authorities responded to our requests. The authorities that did not respond to us were those of Cyprus (Cyprus Radio Television Authority) and Romania (National Authority for Management and Regulation in Communications). We followed up with those authorities that did not reply to us, on 18 April 2024 for the missing DSC from the first batch (Cyprus) and on 22 August 2024 for the missing DSCs of the second batch. The four month interval between April and August was a result of the follow-up being necessary for the two batches of requests. After addressing the missing DSCs from the first batch in April, we had to allow time for the authorities to respond to the second batch before initiating a follow-up in August.

On average, it took the authorities 18.7 days for a first assessment of and response to our requests. The fastest were the DSCs from Italy and Portugal (on the same day), Ireland (one day), Belgium (one day), and Estonia (one day), the slowest were the DSCs from Spain (92 days), Poland (84 days), and Greece (65 days). Most (23) DSCs replied to us in English. Only the DSC from Hungary replied to us in their na-

tional language. The DSC from Slovenia claimed that they could not even process data access requests in English at all because doing so would violate their national laws, more specifically, Article 62 of the Slovenian General Administrative Procedure Act, and prevent future processing of the data access request as its further assessment could potentially represent a substantial violation of administrative procedure requirements.

The responses can be grouped into three categories: 1) DSCs that started working on our request (n= 3), 2) DSCs that refused to process our request (n = 24; nearly all DSCs that responded refused to process our request in the end, with Italy being the only exception, which confirmed receipt without a decision), 3) DSCs that forwarded our request to another DSC (n= 3, including 1 that first said they would process) or merely acknowledged receipt of the request (n= 1). No response was received by 2 DSCs, namely, those of Romania and Cyprus. No successful follow-up attempts were made with those two authorities.

4.1 Started processing of our request

Three DSCs, namely, the Luxembourgish, Swedish, and Maltese authorities announced that they would work on our data access request, which was contrary to all other DSC responses. Nonetheless, all of them issued follow-up responses indicating their inability to process the request. For instance, on 3 April 2024, the Luxembourgish DSC issued a follow-up response indicating that the conditions for granting data access requests are not fully defined yet by the Delegated Act on data access requests, and thus, our request cannot be processed. This indicates legal uncertainty, which poses a challenge for researchers, as they are initially informed that their request is being processed, only to subsequently find that it is not. Additionally, the Luxembourgish DSC highlighted that during the public consultation phase of the Delegated Act in May 2024, stakeholders, including ourselves, will have access to the proposed text of the Delegated Act and can actively participate and contribute to the consultation process. Moreover, the DSC indicated that adjustments to data access requests can be made in accordance with the provisions of the Delegated Act. Rather than simply stating their current limitations, they have outlined actionable steps that researchers can undertake. The

The Swedish DSC and Maltese DSCs also stated in their first email that they would process our application using standard procedures; nonetheless, later on, they informed us that Wikipedia had established itself in the Netherlands and that they cannot continue processing our application.

4.2 Refused to process our request

As for the DSCs that refused to process our request, some stated that they were waiting for legal clarifications before addressing data access requests. The Dutch, the German, and the Czech DSCs (all from the first batch of DARs from 7 March 2024) replied that they were still waiting for the necessary national measures, such as the Dutch Implementation Act regarding the DSA, to operationalise the processing of applications submitted by researchers.

The German authorities refused outright to engage with our data access request, whereas the others promised to proceed once they have the Delegated Act. Another eight DSCs (alongside the Luxembourgish DSC) claimed that they were unable to process our data access request because of the missing Delegated Act by the Commission. For example, in March 2024, the Irish DSC let us know that there will first be a consultation among DSCs on the draft delegation on DARs and then a public feedback request. The DSC specified that this would be followed up by translations and adoption, and it anticipated that the implementation date of the Delegated Act would be in October 2024. As of May 2025, the Commission has published a draft Delegated Act, but its adoption is still not finalised (European Commission, 2023a).

The DSC elaborated that the Delegated Act would not solely establish technical conditions for data provision by VLOPs and VLOSEs but would also prescribe standards for researchers regarding applications, including expectations for DSCs regarding the assessment process (European Commission, 2023b). This effectively implies a suspension of the data access requests instrument until October 2024, representing the primary problem currently hindering the processing of requests. As for the DSCs from the second batch from 26 June 2024 aimed at Wikipedia, 12 DSCs informed us that Wikipedia was now established in the Netherlands and thus we can contact the Dutch DSC, and that they were not responsible. This was, however, not stated on the Commission's website at the time of dispatching the data access requests. Two DSCs, namely, from Latvia and Lithuania informed us that they are not responsible for Wikipedia as it does not yet have an establishment in the EU. The DSCs of Greece and Slovenia merely stated that they are not responsible for data access requests regarding Wikipedia.

4.3 Forwarded our request or merely acknowledged it

In June 2024, we contacted the Croatian, Finnish, and Swedish DSCs, who subsequently informed us that they had forwarded our data access request to the Dutch

DSC, which is now in charge, given Wikipedia's recent establishment in the Netherlands. Notably, the Dutch DSC contacted us stating that they are now the responsible DSC for Wikipedia and that they received multiple emails by other DSCs regarding our data request. Another one, the Italian DSC, merely acknowledged our request but did not provide further information.

4.5 Further observations

Some DSCs advised us on alternative ways of obtaining data, with the Czech DSC standing out for its proactive approach in offering valuable insights on navigating the DSA and highlighting that many platforms already provide APIs for developers and researchers, with further information accessible through the respective websites. An alternative to Article 40 (4) of the DSA was presented by that DSC, namely, access to publicly available data in accordance with Article 40 (12) of the DSA. According to that provision, researchers who meet specific criteria can request access to public data directly from VLOPs and VLOSEs, rather than through the DSCs. Access for such data can be granted through content library or API and does not extend to non-public data as outlined in Article 40 (4) DSA (Coimisiún na Meán, 2025). The Czech DSC also emphasised the value of our feedback regarding the accessibility of XVideos' public data and encouraged us to reach out should any issue arise to this end.

The Austrian DSC, too, was proactive; a member of the authority quickly asked us for a telephone conversation since they have a strong interest in working with academic researchers. The Dutch DSC specified that currently, they can keep our application on file, and as soon as they are authorised to grant applicants the status of vetted researcher, they will start processing our application. Lastly, the Dutch DSC has recognised our right to withdraw our application for data access requests, and the Luxembourgish and Dutch DSCs have recognised our right to make amendments to our data access request. The Bulgarian DSC has also mentioned the Delegated Act as a factor to give more clarity regarding the submission and assessment of applications. This implies that when the Delegated Act is promulgated, and there are technical elements supplementing the requirements for the data access requests, there will be no necessity to submit new requests; rather, the extant ones can be just amended. This presents an opportunity for researchers, as once processing is viable, there could be heightened efficiency in handling the data access requests.

Notably, even after the adoption of the draft Delegated Act, none of the DSCs continued processing our application.

5. Discussion

5.1. Delays in the DSA's Implementation

The DSA represents a significant step towards regulating digital platforms and holding them accountable for systemic risks. Nevertheless, currently, the implementation of its provisions related to data access for vetted researchers is facing serious delays and challenges. One of the most pressing issues is the pending adoption of the Delegated Act on Data Access Requests. Originally, the latter should have been adopted in Spring 2024, according to the Commission. As of Spring 2025, however, the Delegated Act is still not enforced, with only a draft version having been published by the Commission in October 2024. Public consultations were also launched on the draft Delegated Act, with a submission deadline of 10 December 2024. A total of 109 feedback forms were received (European Commission, 2023a).

These delays are critical, as they not only create uncertainty regarding the adoption of the Delegated Act but also hinder researchers' ability to access non-public VLOP and VLOSE's data. Yet, this ability, according to the DSA, is essential for the fundamental rights protection of EU citizens. This delay is especially concerning given the constant spread of illegal content, risk of election manipulation, and the negative impacts on gender-based violence, public health, minors, and a person's physical and mental well-being. An important example is Romania's 2024 presidential election, which drew significant attention due to a candidate's victory in the first round, amid accusations of Russian interference, questionable TikTok activity, and online payments to influencers (Ings, 2025). Beyond electoral interference, VLOPs and VLOSEs are linked to a broader set of risks which must be thoroughly researched in order to be mitigated. Sites like Pornhub continue to raise serious concerns related to gender-based violence and the protection of minors (Mestre-Bach et al., 2024). On the other hand, VLOPs, such as AliExpress and Amazon pose risks to consumer safety, including the potential distribution of counterfeit and unsafe products (Cowley et al., 2020). While it is true that the EU institutions have to balance complex legal and technical frameworks in finalising the Delegated Act and also consider stakeholder feedback, the delay has now stretched beyond a year. Given the constant presence of systemic risks on VLOPs and VLOSEs, it is imperative that these risks are studied and mitigated without further postponement.

5.2. Recommendations and Content of the Delegated Act

Additionally, the question of the content of the Delegated Act arises. Under EU law, Delegated Acts, as per Article 290 of the TFEU, are acts of general application which are meant to supplement or amend non-essential elements of a legislative norms. This means that all the essential elements of data access requests must already be present in the DSA, with the Delegated Act on data access requests supplementing only non-essential elements to Article 40 of the DSA. The draft version of the Delegated Act includes:

"The procedures for Digital Services Coordinators to manage requests and vet researchers and if necessary, the possibility of an independent advisory mechanism in support of providing access to data. The purposes for which the data may be used; The specific conditions for providing researchers with access to data, in particular the provision of access to data in compliance with the GDPR, accounting for the rights and interests of providers of VLOPs and VLOSEs and users concerned, the protection of confidential information and maintaining the security of services and the relevant indicators. The technical conditions under which providers of very large online platforms and very large online search engines are to provide access to data to the Commission and the Digital Services Coordinators of establishment and with vetted researchers." (European Commission, 2023a)

The question of whether the aforementioned conditions of the Delegated Act are purely non-essential technical and procedural elements which supplement the DSA, remains to be answered. It may lead to legal challenges from tech companies, arguing that the Commission has overstepped its competences in drafting and applying the Delegated Act.

In addition to that, the authors of this paper together with researchers from Maastricht University, University of Lausanne, the University of St. Gallen, and the University of Oxford, have submitted a response to the public consultation on the draft Delegated Act (Consortium of Researchers from Maastricht University, University of Lausanne, University of St. Gallen and University of Oxford, 2024). In our response, we scrutinised the content of the draft Delegated Act and identified notably gaps. In particular, we found that the mediation mechanism proposed by the draft Delegated Act in Article 13 should be revised to address current limitations. In addition to that, the mediation mechanism proposed in Article 13 of the draft Delegated Act should be revised to address several limitations. As currently formulated, the mediation process is limited to addressing amendments to data access requests and does not extend to verifying whether the requested data has been

provided accurately and within the required timeframe. Moreover, there are legitimate concerns about the impartiality of the mediation procedure, as the data provider is responsible for both selecting and funding the mediator. This arrangement, as outlined in Article 13, risks undermining the neutrality and fairness of the mediation process. To improve transparency and trust, the European Commission could establish a pool of independent mediators who have no financial or personal affiliations with either party. Mediators could then be randomly assigned from this list when mediation is initiated. Alternatively, both parties the data provider and the Digital Services Coordinator could jointly select a mediator from a Commission-approved list, ensuring a more balanced and equitable process.

We also recommend the timely establishment of a centralised point of contact for the submission of data access requests, such as the Data Access Portal proposed by the draft Delegated Act , accompanied by guidelines ensuring timely data access for researchers, and underpinned by sanctions for noncompliance with those timelines for DSCs and VLOPs. Furthermore, the framework of data access requests should include a mechanism enabling researchers to track the real-time status of their applications. Moreover, there is a need to provide training for DSCs on effectively managing data access requests. Notably, instances such as the Luxembourgish DSC initially committing to processing our application, only to retract it later, underscore the necessity for enhanced procedural clarity. Furthermore, the EU should facilitate the secure storing of data by researchers who lack the necessary capacity to ensure data safety, thereby removing the burden from individual researchers and enhancing data protection (Engler, 2021).

Overall, the absence of mechanisms to ensure that researchers receive qualitative and complete data in a timely manner risks introducing further delays and hurdles to researchers receiving the data that they should under the DSA once the Delegated Act is adopted.

5.3. Delays in National Adoption

Furthermore, one can observe notable delays in the enactment or pending adoption of national legislation pertinent to the DSA in Germany, the Netherlands, and the Czech Republic, among others (European Commission, 2024a). This, in turn, impedes the establishment of capable national DSCs. These delays matter because the initial phase of the data access requests relies on the DSC's scrutiny. Of particular concern is the failure to meet the deadline for appointing a DSC, as stipulated by the DSA, which was the 17 February 2024. For instance, the Dutch DSC, responded to our data access request that they cannot handle our application yet

due to lack of national measures enacting the DSA. According to that DSC, the timeline for its implementation remains uncertain, contingent upon legislative decisions in the Dutch jurisdiction, potentially being finalised even later than the Delegated Act. On 7 May 2025, the Commission referred Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union for failing to designate and/or empower a DSC (European Commission, 2025).

5.4. Harmonisation of the Data Access Request Procedure

This further leads to the question of harmonisation of the data access request procedure among all DSCs. Although all the authorities that responded ultimately concluded that they could not process the data access request, their responses varied significantly in terms of timing, communication formats, legal reasoning, and level of engagement. While the DSA is an EU regulation and aims to establish a consistent regulatory framework across the EU, discrepancies in its implementation already exist and may deepen over time

This could potentially create an uneven playing field for researchers and impact the quality and comparability of research findings, as they might face different timelines, requirements, and obstacles depending on the country, complicating their efforts to study systemic risks. For instance, while certain DSCs, like the Irish one, demonstrate efficiency by promptly responding within a day, others, like the DSC of Cyprus, have not responded to any of the requests forwarded to them.

6. Conclusions

This paper serves as the foundation for future research on data access requests by creating and sending such requests for non-public VLOP data to all 27 DSCs across the EU member states. In doing so the paper aimed to understand the current implementation of Article 40(4) of the DSA.

From the responses to our data access requests, we found that the operationalisation of Article 40(4) of the DSA has been effectively stalled for more than a year. As of late September 2024, all DSCs that responded to us indicated that they are unable to process our requests for non-public data from the respective VLOPs in their countries. While the specific reasons vary between the DSCs, the underlying issue is the continued delay of an adopted Delegated Act.

Various other factors contribute to the current lack of implementation of Article 40(4) of the DSA across the examined DSCs. This ranges from delays in the enactment of legislation establishing a functional DSC in member states, failing to meet

the deadline to appoint a DSC, namely 17 February 2024, and to differing response times. Some DSCs even refused to communicate with us in English, even though VLOPs or VLOSEs usually operate across EU borders and beyond. Being open to scrutiny from researchers across the globe is therefore important, and the ability to file data access requests in English should be an important precondition for effective scrutiny of platforms through researchers. Nonetheless, such a procedural right is not guaranteed by EU law and indeed the draft Delegated Act in Article 6 states that DSCs shall indicate the Union languages in which they will accept data access requests. This paper argues that, unlike other national authorities applying national law, DSCs' establishment is mandated by EU law and those are tasked with enforcing EU law. Accordingly, the DSCs can adopt good administrative practices by accepting requests in English, alongside their national language, to facilitate the equitable access for researchers all across the Union.

In conclusion, although this study set out to assess the operationalisation of Article 40(4) of the DSA, the findings instead revealed an early phase which is characterised by legal uncertainty in the adoption of the Delegated Act as well as fragmented preparedness and procedural delays among DSCs. Notably, all DSCs that responded refrained from interpreting and applying the law. While Article 40(4) of the DSA offers a promising path for vetted researchers to access non-public data from VLOPs and VLOSEs to study systemic risks online, its effectiveness depends on the timely and coordinated establishment of legal and procedural infrastructure to support its operationalisation. Moving forward, our research will continue after the implementation of the Delegated Act, trying to create a comprehensive analysis of the entire data access request process across the involved countries.

References

Albert, J. (2022). *A guide to the EU's new rules for researcher access to platform data*. Algorithm Watch. https://algorithmwatch.org/en/dsa-data-access-explained

AlgorithmWatch. (2024). *Online systemic risks under the DSA: Crowdsourced evidence*. https://eu.jotform.com/form/233514485703052

Bekavac, L., Garcia, K., Strecker, J., Mayer, S., & Tamò-Larrieux, A. (2024). *From walls to windows: Creating transparency to understand filter bubbles in social media*. https://www.alexandria.unisg.ch/server/api/core/bitstreams/25369dea-08e2-4cde-811f-2edcab111b6f/content

Bird & Bird. (2024). *Digital Services Act tracker and UK Online Safety Act*. Bird & Bird. https://www.twobirds.com/en/trending-topics/digital-services-act-tracker-and-uk-online-safety-act

Brown, M. A. (2023). *The problem with TikTok's new researcher API is not TikTok*. Tech Policy Press. https://www.techpolicy.press/the-problem-with-tiktoks-new-researcher-api-is-not-tiktok/

Coimisiún na Meán. (2025). *Vetted researcher data access*. Coimisiún Na Meán. https://www.cnam.ie/industry-and-professionals/online-safety-framework/certifications-schemes/vetted-researchers/

Consortium of Researchers from Maastricht University, University of Lausanne, University of St. Gallen and University of Oxford. (2024). *Feedback from: Consortium of Researchers from Maastricht University, University of Lausanne, University of St. Gallen and University of Oxford*. (Feedback No. F3498690). European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act/F3498690_en

Cowley, J., Tomlinson, A., & Vellani, N. (2020). *Why you might want to think twice before shopping online: We bought dozens of products from AliExpress, Amazon, eBay, Walmart and Wish. Over half were suspected fakes*. CBC News. https://www.cbc.ca/news/business/marketplace-counterfeits-fakes-online-shopping-1.5470639

Darius, P., & Stockmann, D. (2023). *Implementing data access of the Digital Services Act* [Policy Brief]. Hertie School. https://opus4.kobv.de/opus4-hsog/frontdoor/deliver/index/docId/4947/file/Implementing_Data_Access_Darius_Stockmann_2023.pdf

Datta, A. (2025). *WhatsApp to get added EU scrutiny*. Euractiv. https://www.euractiv.com/section/tech/news/whatsapp-to-get-added-eu-scrutiny/

DSA Observatory. (2024). *About*. DSA Observatory. https://dsa-observatory.eu/#top

Eder, N. (2023). Making systemic risk assessments work: How the DSA creates a virtuous loop to address the societal harms of content moderation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4491365

Engler, A. (2021). *Platform access is a lynchpin of the EU's Digital Services Act*. Brookings. https://www.brookings.edu/articles/platform-data-access-is-a-lynchpin-of-the-eus-digital-services-act/

European Commission. (2023a). *Delegated regulation on data access provided for in the Digital Services Act*. European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en

European Commission. (2023b). *Digital Services Act: Summary report on the call for evidence on the Delegated Regulation on data access*. Digital Strategy. https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-call-

evidence-delegated-regulation-data-access

European Commission. (2024a). *Digital Services Coordinators*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs

European Commission. (2024b). *Supervision of the designated very large online platforms and search engines under DSA*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-slops

European Commission. (2025). *Commission decides to refer CZECHIA, SPAIN, CYPRUS, POLAND and PORTUGAL to the Court of Justice of the European Union due to lack of effective implementation of the Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081

European Digital Media Observatory. (2022). *Report of the European Digital Media Observatory's working group on platform-to-researcher data access*. https://edmo.eu/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

European Union. (2025). *Illegal content on online platforms*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/illegal-content-online-platforms

Flew, T., & Martin, F. (Eds.). (2022). *Digital platform regulation: Global perspectives on internet governance*. Palgrave Macmillan.

German Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support. (n.d.). *Datenzugang für die Forschung* [Deutsches Zentrum für Cyber-Sicherheit]. DSC Bund. https://www.dsc.bund.de/DSC/DE/6Forschung/start.html

Goanta, C., Zannettou, S., Kaushal, R., van de Kerkhof, J., Bertaglia, T., Annabell, T., Gui, H., Spanakis, G., & Iamnitchi, A. (2025). *The great data standoff: Researchers vs. platforms under the Digital Services Act* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2505.01122

Grevy Gotfredsen, S., & Dowling, K. (2024, July 9). *Meta is getting rid of CrowdTangle—And its replacement isn't as transparent or accessible*. Columbia Journalism Review. https://www.cjr.org/tow_center/meta-is-getting-rid-of-crowdtangle.php

Hohlfeld, A. (2025). *DSA: Risk assessment & audit database*. Google Spreadsheets. https://docs.google.com/spreadsheets/d/12hJWpCFmHJMQQlz1qkd6OgGsMW82YcsWgJHXD7BHVps/edit?gid=0#gid=0

Ings, R. (2025). *The TikTokers accused of triggering an election scandal*. BBC. https://www.bbc.com/articles/cqx41x3gn5zo

Jaursch, J. (2022). *Platform oversight*. Verfassungsblog. https://verfassungsblog.de/dsa-dsc/

Jaursch, J. (2024). *The Digital Services Act is in effect-Now what?* Stiftung Neue Verantwortung. https://www.stiftung-nv.de/en/publication/digital-services-act-now-what

Kira, B. (2024). Pro-competition and online safety: A more holistic approach to digital platform regulation. *SSRN Electronic Journal*. https://ssrn.com/abstract=4631357

Kollnig, K., & Shadbolt, N. (2023). *How decisions by Apple and Google obstruct app privacy*. Technology and Regulation (TechReg.

Leerssen, P. (2021). Platform research access in Article 31 of the Digital Services Act. In *To break up or regulate big tech? Avenues to constrain private power in the DSA/DMA package*. https://ssrn.com/abstract=3932809

Marsh, O. (2024). *Got complaints? Want data? Digital service coordinators will have your back – or will they?* Algorithm Watch. https://algorithmwatch.org/en/dsa-day-and-platform-risks/

Mestre-Bach, G., Villena-Moya, A., & Chiclana-Actis, C. (2024). Pornography use and violence: A systematic review of the last 20 years. *Trauma, Violence, & Abuse*, *25*(2), 1088–1112. https://doi.org/10.1177/15248380231173619

Miller, G. (2023). *Tracking the first Digital Services Act transparency reports*. Tech Policy Press. https://www.techpolicy.press/tracking-the-first-digital-services-act-transparency-reports

Miller, G. (2024). *European Commission issues report on researcher access to online platform data*. Tech Policy Press. https://www.techpolicy.press/eu-commission-report-researcher-access-platform-data/

Murtfeldt, R., Alterman, N., Kahveci, I., & West, J. D. (2024). *RIP Twitter API: A eulogy to its vast research contributions*. arXiv. https://doi.org/10.48550/ARXIV.2404.07340

Swan, E. J. (2022). *Internet law: A concise guide to regulation around the world*. Kluwer Law International.

Synodinou, T. H., Jougleux, P., Markou, C., & Prastitou, T. (Eds.). (2020). *EU internet law in the digital era: Regulation and enforcement*. Springer.

Van Drunen, M. Z., & Noroozian, A. (2024). How to design data access for researchers: A legal and software development perspective. *Computer Law & Security Review*, *52*. https://doi.org/10.1016/j.clsr.2024.105946

Van Hoboken, J., Quintais, J. P., Appelman, N., Fahy, R., & Buri, I. (2023). *Putting the Digital Services Act into practice: Enforcement, access to justice, and global implications* (M. Straub, Ed.). Verfassungsbooks.

Wilman, F. (2022). The Digital Services Act (DSA)—An overview. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4304586

Annex: Example of a data access request

Note that the data access requests discussed within this study were created solely based on the requirements set out in Article 40(4)–(11) of the DSA, since the Delegated Act on data access requests, which will supplement those requirements, was not in force yet.

Sent to: Autoriteit Consument en Markt

Address: 2500 BH The Hague

Point of contact with the authority: acm-post@acm.nl

Subject: Data Request

March 2024

To whom it may concern,

Based on Article 40 of the Digital Services Act (DSA) I make use of my right to data access.

Vetted researchers

In accordance with Article 40(8) DSA and Article 2, point (1), of Directive (EU) 2019/790, I am a 'vetted researcher' working at the University X which can be verified in Annex I. In my research lab, we are conducting independent research that is not commercially motivated. The funding for this research comes fully from our public research university. We also included a data management plan, outlined in Annex II, to ensure that the data received is adequately secured and that confidentiality is respected insofar as such security and confidentiality measures are necessary and proportionate for the intended research. We commit to making our research results publicly available free of charge within a reasonable period after the completion of the research, in accordance with Regulation (EU) 2016/679.

Research

The types of requested data can be identified in Annex III. The research question of the paper is: *What are the challenges and opportunities in obtaining data from*

different VLOPs located in different countries (in the case study of understanding illegal content on their platforms)? Hence, the data received through the request will contribute to the detection, identification and understanding of systemic risks pursuant to Article 34(1) DSA, in particular in relation to the dissemination of illegal content. This is crucial because certain forms of illegal content remain absent from the Transparency Reports of AliExpress, hindering a comprehensive assessment of systemic risks within the Union, as stipulated in Article 34(1) of the DSA. Although these reports offer insights into the presence of illegal content, they fall short in providing a detailed breakdown of such content based on groupings and distinctive characteristics. Furthermore, the reports do not address the number of illegal content taken down for different periods of time, hindering the analysis conducted by researchers regarding illegal content patterns and developments.

To address this gap, the disclosure of the requested data is essential. The requested data with regards to user interaction and geographic information is also essential for the understanding of systemic risks in different countries and the user interaction with this content. This information is essential for understanding systemic risks for several reasons: regional variation in illegal content, analysing cultural sensitivity, and identification of emerging threats. Furthermore, as the Platforms Risk Assessments are still not publicly available, and it is not clear what insights those assessments will offer, such information is crucial for the purposes of this research. This is also exemplified by the fact that only the Commission will have access to the full version of the risk assessments.

Lastly, the research will contribute to the assessment of adequacy, efficiency and impacts of the risk mitigation measures taken under Article 35 DSA by assessing measures implemented by VLOPs to mitigate the identified systemic risk. For instance, the requested data regarding “trusted flaggers” based on the category of illegal content is essential for assessing the mitigation measures taken by AliExpress. The same applies in relation to the data requested with regards to the median time and tools for content moderation of content depending on the categorisation provided by the VLOP.

Moreover, this research aims to analyse the responses of various VLOPs located in different countries. The objective is to assess the opportunities and challenges faced by vetted researchers when seeking data from these VLOPs. Therefore, the data requested will also be a pretext in research on monitoring the effectiveness of Article 40 DSA, and the platforms’ willingness to abide by it and fully collaborate with researchers to monitor systemic risks. By doing so, the research seeks to provide valuable insights into the effectiveness of measures taken by platforms, contributing to a more comprehensive understanding of the landscape of illegal content moderation.

Data request

In accordance with the aforementioned research objectives and Article 40 of the DSA, we hereby request the data specified in Annex III. It is important to note, that the requested data are both necessary for, and proportionate to, the purposes of this research as the data requested from AliExpress is detailed data on illegal content. Our request is carefully tailored to align with the research objectives, demonstrating a commitment to avoid any unnecessary intrusion into personal or sensitive information unrelated to our study. The requested data spans the period from 2018 to 2024, a time frame selected with careful consideration as not too short and not too long for our intended research. It's imperative to note that this data is not publicly available, nor is it included in Transparency reports. The necessity of our request stems from the absence of less intrusive alternatives to obtain this critical information. The nature of the data requested, focusing on data related to illegal content, ensures that we steer clear of personal or sensitive data as well as trade secrets. Moreover, this approach is pivotal for the success of our research, as assessing systemic risks in the EU related to illegal content hinges on understanding specific categories and their content moderation.

The research, aiming to explore the challenges and opportunities in obtaining data on illegal content from different platforms, would be rendered ineffective without access to the specified data. Furthermore, the research aims to analyse the differences and similarities in the nature of illegal content between the different VLOPs. This is crucial in analysing how the same systemic risk can be potentially different on various platforms, which in itself, would contribute significantly to the public interest and future policy proposals. We believe the requested data is proportionate to our aims, as the benefits derived from analysing and understanding online illegal content far outweigh any potential drawbacks of data retention by these platforms. The requested data is not personal or sensitive but rather statistical, intending to contribute to the effective monitoring and comprehension of online illegal content, emphasising its significance.

Furthermore, you may not reject this data access request in order to safeguard trade secrets or commercial interests pursuant to Article 40(5)(b) of the DSA. Firstly, the Trade Secrets Directive underscores that confidentiality can be maintained if reasonable measures are in place to protect the information. This data request has implemented such reasonable measures through the implementation of a data management plan, as detailed in Annex II. Secondly, the requested information is not unduly burdensome to invoke a rejection under commercial interests, as the types of data explicitly align with the permitted requests outlined in Recital 97. Therefore, access to the information sought in this data access request should be granted.

In conclusion, we respectfully request access to the relevant data as per the conditions set forth in Art. 40 of the DSA. We believe that our research activities align with the goals of the DSA, and the information obtained will contribute

significantly to the advancement of knowledge in the specified areas.

Sincerely,

X

Annex I: Proof of Employment by a University

Here a proof of employment from the University was declared to the DSCs.

Annex II: Data management plan

The following Data Management Plan (DMP) was drafted in consultation with the Coordinator of Data Stewardship Services and Data Steward to the Faculty of Science and Engineering as well as the Data Steward to the Faculty of Law from University X.

The data obtained from the data access requests will be stored in secure data storage provided by University X and in line with the rules under University's Data Management Code of Conduct. The raw data will only be handled and analysed by researchers who are directly affiliated with the research project. The results arising from the analysis will only be released insofar as is necessary for the purposes of scientific publications and in line with the stated research aims relating to systemic risks. In all stages of the project, any data will be handled in a confidential manner.

Once the project has been completed, and in accordance with the University's Data Management Code of Conduct, the data will be stored and archived in the infrastructure facilities made available by the university at the end of the research project (or earlier, depending on the relevant faculty guidelines or other applicable rules). To the extent that long-term storage is not required by a law, rule, contract, subsidy, or faculty guideline, all research results must be stored for a period of at least ten years after the final publication of the relevant data.

The University's Data Management Code of Conduct, the faculty data management protocol, and the storage environment have all been approved by the data protection officer of the university.

Annex III: The requested data

The request refers to data which is available between 2018-2024. This is because the research aims to provide the public with comprehensive information about illegal content online, capturing the evolving landscape of such content.

In the AliExpress Transparency Report, there is data on violation distribution of moderated content about IP infringements (12%), scams and fraud (10%), unsafe and illegal products (73%), scope of platform services (4%), other (1%). As these

statistics pertain to illegal content, which represents a systemic risk under the DSA, it is crucial for research purposes that VLOPs be more transparent and provide a more detailed breakdown of illegal content. This transparency is essential for aiding academic research, informing policy development, mitigating risks, raising public awareness, and ultimately contributing to a safer online environment.

We request data on the percentages of a more detailed breakdown of all the different categories of illegal content on AliExpress. More specifically, we request data on:

- What are all the types of IP infringements (by categories of goods, e.g. watches, jewellery, handbags), the types of scams and fraud (e.g., non-delivery of products and "fake reviews"), and the categorisation of unsafe and illegal products (e.g., categories such as narcotics and explosives). Concerning the "others" category, we kindly request clarification regarding its contents and, specifically, detailed information on specific percentages attributed to each sub-category.
- The number of illegal content taken down annually from 2018 until 2024 for each categorisation.
- The number of notices submitted by trusted flaggers (since February 17th, 2024), as this is crucial for the assessment of systemic risks' mitigation and also it is information which must be present in the VLOPs Transparency Report, as per Article 15(1)(b) DSA. However, as the obligation was still not in force, when the first transparency reports were launched, we request the data.
- The categorisation of the trusted flaggers' notices based on the specific category of illegal content.
- The data on the time it takes to take down such illegal content, as per category. Namely, data on the median time for taking the different types of categories down, based on automatic or non-automatic tools.
- Data with regards to user interaction with illegal content as per categorisation on your platform. This refers specifically to the number of views for products that may be associated with illegal items, in order to analyse which content attracts the most attention and whether there are any trends overtime.
- Lastly, we request data on geographic information. More specifically, we request data on the geographic location associated with the upload or creation of illegal content as per category, as this would advance the research on mitigating systemic risks. Platforms and the public, armed with knowledge of the source of problems, can centralise their efforts to mitigate risks effectively.

Published by

Alexander von Humboldt
Institute for Internet and Society

in cooperation with

University of Tartu
Johan Skytte Institute of
Political Studies